XACT DATA DISCOVERY
Because you need to know

Digital Forensics Report

UNITED STATES OF AMERICA
v.
ROBERT T. BROCKMAN

Cr. No. 4:21cr 009 GCH

XDD Report 30237-1

August 5, 2021

Prepared by:
Scott Polus – *Regional Vice President, Forensic Services*
Xact Data Discovery
12801 North Central Expressway
Suite 250
Dallas, Texas 75243

US v. Brockman
DX-32
Case No: 4:21-cr-0009

Introduction

1. I am the Regional Vice President of Forensics Services for Xact Data Discovery ("XDD"). I have managed, trained in, and performed various digital forensic analyses with XDD for over 14 years. XDD is a leading provider of electronic discovery ("eDiscovery") and digital forensic services, including the collection, preservation, processing, and analyzing electronically stored information ("ESI").

2. I am a Certified Computer Examiner (CCE) through the International Society of Forensic Computer Examiners (ISFCE). I receive ongoing training in various facets of digital forensics, including mobile devices, personal computer operating systems, cloud-based services, and other related areas. Additionally, I provide continuing education (CLEs), webinars, articles, and training regarding the same for law firms and various professional legal organizations and seminars.

3. I have previously provided testimony and was admitted as a computer forensics expert in Federal and State Courts.

Background

4. Jones Day asked XDD to analyze a subset of documents from a laptop and report on the documents' metadata

5. XDD analyzed a Dell Precision M6800 laptop with a unique Service Tag of 5L84V32 (the "Laptop"). The entire physical storage device in the Laptop—a 500 GB Samsung SSD 860 EVO mSATA, having a serial number of S41NNB0KC05315L (the "Hard Drive")—was successfully preserved on Thursday, October 22, 2020, when a forensic image was taken of the Hard Drive (the "Forensic Image").

6. The Message Digest 5 (MD5) hash is commonly used for integrity verification in the forensic imaging process. Hashing refers to the use of a cryptographic hash function to compute a unique value for a data set to verify that the forensic image is identical to the source. The MD5 hash value computed from the Hard Drive matched the value computed for the Forensic Image- eaa09abda7dfa7071a5e362e515ec8e2. This validates that the data within the Forensic Image is identical to the data on the Hard Drive.

7. A backup (or working copy) of the Forensic Image was created and successfully verified as an exact copy using the same MD5 hashing algorithm (the "Working Copy"). This allows the Working Copy to be authenticated at any time by another expert should the need arise. My analysis was conducted on the Working Copy.

Analysis

8. Counsel identified a total of fifteen documents for examination from the Laptop. All 15 of these documents ("Health Issues Documents") were within with [ROOT]\BOBDOC2\healthdoc\ directory and had the following filenames:

i. HEALTH ISSUES DECEMBER 2004.doc
ii. HEALTH ISSUES DECEMBER 2005.doc
iii. HEALTH ISSUES DECEMBER 2006.doc
iv. HEALTH ISSUES DECEMBER 2007.doc
v. HEALTH ISSUES DECEMBER 2008.doc
vi. HEALTH ISSUES DECEMBER 2009.doc
vii. HEALTH ISSUES DECEMBER 2010.doc
viii. HEALTH ISSUES DECEMBER 2011.doc
ix. HEALTH ISSUES DECEMBER 2012.doc
x. HEALTH ISSUES DECEMBER 2013.doc
xi. HEALTH ISSUES DECEMBER 2014.doc
xii. HEALTH ISSUES DECEMBER 2017.doc
xiii. HEALTH ISSUES SEPTEMBER 2015.doc
xiv. HEALTH ISSUES SEPTEMBER 2016.doc
xv. HEALTH ISSUES SEPTEMBER 2018.docx

9. The export of the underlying metadata contained the following metrics from the Health Issues Documents:

Metadata Excerpt for Health Documents

Filename	Doc Year	Created Date	Last Modified Date	Last Saved Date	Revision Number	Words	Characters
HEALTH ISSUES DECEMBER 2004.doc	2004	12/14/2004	12/14/2004	12/14/2004	1	104	595
HEALTH ISSUES DECEMBER 2005.doc	2005	12/12/2005	12/12/2005	12/12/2005	2	292	1665
HEALTH ISSUES DECEMBER 2006.doc	2006	12/2/2006	12/2/2006	12/2/2006	2	253	1446
HEALTH ISSUES DECEMBER 2007.doc	2007	12/9/2007	12/9/2007	12/9/2007	2	300	1710
HEALTH ISSUES DECEMBER 2008.doc	2008	12/1/2008	12/1/2008	12/1/2008	2	447	2549
HEALTH ISSUES DECEMBER 2009.doc	2009	12/13/2009	12/13/2009	12/13/2009	2	714	4075
HEALTH ISSUES DECEMBER 2010.doc	2010	12/13/2010	12/13/2010	12/13/2010	2	815	4652
HEALTH ISSUES DECEMBER 2011.doc	2011	12/17/2011	12/17/2011	12/17/2011	2	921	5254
HEALTH ISSUES DECEMBER 2012.doc	2012	12/7/2012	12/7/2012	12/7/2012	2	945	5387
HEALTH ISSUES DECEMBER 2013.doc	2013	12/17/2013	12/17/2013	12/17/2013	2	829	4730
HEALTH ISSUES DECEMBER 2014.doc	2014	12/16/2014	12/16/2014	12/16/2014	2	826	4711
HEALTH ISSUES SEPTEMBER 2015.doc	2015	9/29/2015	9/29/2015	9/29/2015	2	1244	7095
HEALTH ISSUES SEPTEMBER 2016.doc	2016	11/13/2016	11/13/2016	11/13/2016	2	1604	9146
HEALTH ISSUES DECEMBER 2017.doc	2017	1/13/2018	1/13/2018	1/13/2018	2	1654	9429
HEALTH ISSUES SEPTEMBER 2018.docx	2018	8/27/2018	8/27/2018	8/27/2018	1	355	2030

10. The metadata for each document shows that the year contained within each of the filenames is within a month or two of each document's Created Date. Further, each document's Created Date, Last Saved Date, and Last Modified Date are an exact match. This match between the Created, Last Saved, and Last Modified Dates indicates that these documents were not modified after the day they were created.

11. Starting with the oldest document created in December 2004, the Revision Number shows that this is the first iteration of that file, and it was created and last saved on 12/12/2004.

12. In December 2005, the user modified the previous year's document and saved a copy with the then-current year (2005) in the filename again. The first time the user "saved-as" this new file, it reset the Revision Number to 1. After the user made modifications to the document and saved it, this increased the Revisions Number to 2.

13. The Revision Number usually only increments when one opens a document and "saves on closing." If one chooses to manually save (not the "Save-As" option) a document, the Revision Number doesn't always increment until it is fully closed. When one chooses to

"Save-As" from within Microsoft Word, the Revision Number resets to 1.

14. The user continued this pattern of saving a new copy of the previous year's document with the updated year in the filename through to the December 2017 version of the document (created on 1/13/2018).

15. The metadata and content suggests that the final version of the Health Issues Document, created on 8/27/2018, was not saved from the previous year's document. Instead, it appears that the user created this document from scratch.

Conclusions

16. The user's annual updates to the Health Issues Documents are consistent with the habit of a user taking a previous version of a document to seed a subsequent and related document.

17. Each Health Issues Document has a filename that matches or closely matches the document's Created Date.

18. The Health Issues Documents' Created, Last Modified, and Last Saved Dates show that no further modifications were made to these documents after the day they were created.

X

Scott Polus
RVP - Forensics Services